

THE PREDICTABLE DEGREE PROPERTY, COLUMN REDUCEDNESS, AND MINIMALITY IN MULTIDIMENSIONAL CONVOLUTIONAL CODING

VAKHTANG LOMADZE*

Abstract. Higher-dimensional analogs of the predictable degree property and column reducedness are defined, and it is proved that the two properties are equivalent. It is shown that every multidimensional convolutional code has, what is called, a minimal reduced polynomial resolution. It is uniquely determined (up to isomorphism) and leads to a number of important integer invariants of the code generalizing classical Forney's indices.

Key words. Convolutional code, filtered module, PD property, polynomial resolution, reduced polynomial resolution, graded module, column degree table, Forney table.

1. Introduction. Multidimensional convolutional codes are natural generalizations of classical (one-dimensional) convolutional codes and are used to transmit multidimensional data. They have been studied quite a bit in the literature and we refer the reader to Fornasini and Valcher [4], Valcher and Fornasini [15], Weiner [16] and more recent works Charoenlarnnopparut [1], Gluesing-Luerssen et al. [6], Jangisarakul and Charoenlarnnopparut [7], Kitchens [8], Napp Aveli et al. [13, 14], Zerz [17].

In this article, we would like to offer a new view-point on some fundamental issues of algebraic character related to multidimensional convolutional codes.

Throughout, \mathbb{F} is an arbitrary (finite) field, n a fixed positive integer, and $D = (D_1, \dots, D_n)$ a sequence of indeterminates. We let $S = \mathbb{F}[D]$. For every $d \in \mathbb{Z}$, we shall write $S_{\leq d}$ to denote the space of polynomials of degree $\leq d$.

Following Weiner [16] and other authors, by a convolutional code of length q we mean a submodule of S^q . If C is a convolutional code of length q , then, for each $d \geq 0$, define $C_{\leq d} = C \cap S_{\leq d}^q$ to be the space of codewords of degree $\leq d$.

In dimension 1, a submodule $C \subseteq S^q$ is free, and it is possible therefore to represent it via a full column rank polynomial matrix. In other words, there exist an integer p and a polynomial matrix $G \in S^{q \times p}$ such that

$$0 \rightarrow S^p \xrightarrow{G} C \rightarrow 0$$

is an exact sequence. A higher-dimensional counterpart of this well-known fact is Hilbert's syzygy theorem, according to which there exists $1 \leq l \leq n$, and there exist integers $p_1, \dots, p_l \geq 1$ and polynomial matrices G_1, \dots, G_l of sizes $q \times p_1, \dots, p_l \times p_{l-1}$, respectively, such that the sequence

$$0 \rightarrow S^{p_l} \xrightarrow{G_l} S^{p_{l-1}} \rightarrow \dots \rightarrow S^{p_1} \xrightarrow{G_1} C \rightarrow 0$$

is exact. This celebrated theorem suggests to define higher-dimensional analogs of classical full column rank polynomial matrices as sequences (G_l, \dots, G_1) of polynomial matrices satisfying the above exactness condition.

Starting with this idea, we shall define higher-dimensional analogs of the predictable degree property and column reducedness, and prove that the two properties are equivalent. We shall see that every multidimensional convolutional code has, what

*A. Razmadze Mathematical Institute, Mathematics Department of I. Javakhishvili State University, Georgia (vakhtang.lomadze@tsu.ge).

we call, a minimal reduced polynomial resolution. It is uniquely determined (up to isomorphism) and provides a number of important integer invariants of the code that generalize classical Forney's indices.

Recall that the degree of a column f with entries in S is defined to be the maximum of the degrees of the components of f ; it is denoted by $\deg(f)$. We shall need *relative* degrees as well. Any function $[1, p] \rightarrow \mathbb{Z}_+$ will be referred to as a twisting (or degree) function of length p . If a is a twisting function of length p , then, for $f \in S^p$, we set

$$\deg_a(f) = \max_i \{a(i) + \deg(f_i)\}.$$

(If f is zero, then $\deg_a(f) = -\infty$.) Notice that $\deg(f) = \deg_0(f)$.

Without loss of generality, we shall always consider polynomial matrices with no zero column. For such matrices, we can define (column) degree functions. The degree function of a polynomial matrix $G \in S^{p \times q}$, denoted by $\deg(G)$, is the function that assigns to every $j \in [1, q]$ the degree of the j -th column of G . More generally, if a is a twisting function of length p , we define the a -degree function $\deg_a(G) : [1, q] \rightarrow \mathbb{Z}_+$ to be the function that assigns to every $j \in [1, q]$ the a -degree of the j -th column of G . This is a degree function of length q .

By a polynomial complex of length l , we shall mean a sequence (G_l, \dots, G_1) of polynomial matrices, such that the products $G_1 G_2, \dots, G_{l-1} G_l$ (are defined and) are zero. The size is defined to be $q \times (p_l, \dots, p_1)$, where q is the row number of G_1 and p_1, \dots, p_l are the column numbers of G_1, \dots, G_l . We say that (G_l, \dots, G_1) is a polynomial resolution if

$$0 \rightarrow S^{p_l} \xrightarrow{G_l} S^{p_{l-1}} \rightarrow \dots \rightarrow S^{p_1} \xrightarrow{G_1} S^q.$$

is an exact sequence.

If C is a convolutional code, then, as already said, Hilbert's syzygy theorem guarantees existence of a polynomial resolution (G_l, \dots, G_1) such that $\text{Im}(G_1) = C$. The number l , called the homological dimension of C , is an important integer invariant of C . This number measures the complexity of C and indicates how far is C from being free. Free convolutional codes are exactly convolutional codes of homological dimension 1.

The point of convolutional codes is that they admit a natural *homogenization*, and this permits us to study them using the method of graded modules. We introduce an extra ("homogenizing") indeterminate D_0 , and define $T = \mathbb{F}[D_0, D]$. Given an integer function $a : [1, p] \rightarrow \mathbb{Z}$, we shall write D_0^a for the diagonal matrix with $D_0^{a(1)}, \dots, D_0^{a(p)}$ on the diagonal.

This article has much overlaps with [11]. The relevant results from [11] are reproduced in a rather sketched form. The main new contribution is Theorem 1, which generalizes Forney's classical theorem stating that a full column rank polynomial matrix has the predictable degree property if and only if its leading coefficient matrix has full column rank.

2. Filtered modules, and the PD property. Let M be a module over S . A filtration on M is an ascending chain

$$M_{\leq 0} \subseteq M_{\leq 1} \subseteq M_{\leq 2} \subseteq \dots$$

of linear subspaces of M such that

$$M = \bigcup M_{\leq d} \quad \text{and} \quad D_k M_{\leq d} \subseteq M_{\leq d+1} \quad \forall k, d.$$

A module equipped with a filtration is called a filtered module.

A twisting function $a : [1, p] \rightarrow \mathbb{Z}_+$ determines on S^p a filtration consisting of the spaces

$$S^p[-a]_{\leq d} = \{f \in S^p \mid \deg_a(f) \leq d\} \quad (d \geq 0).$$

The module S^p equipped with this filtration is denoted by $S^p[-a]$. Given a submodule $C \subset S^p$, we shall write $C[-a]$ to denote the module C together with the filtration induced from $S^p[-a]$, that is,

$$C[-a]_{\leq d} = C \cap S^p[-a]_{\leq d}.$$

A homomorphism of filtered modules $(M, (M_{\leq d})) \rightarrow (N, (N_{\leq d}))$ is a homomorphism $u : M \rightarrow N$ such that

$$\forall d \geq 0, \quad u(M_{\leq d}) \subseteq N_{\leq d}.$$

Example. If $a : [1, p] \rightarrow \mathbb{Z}_+$ and $b : [1, q] \rightarrow \mathbb{Z}_+$ are two functions, then

$$\text{Hom}(S^q[-b], S^p[-a]) =$$

$$\{(g_{ij}) \in S^{p \times q} \mid \deg(g_{ij}) \leq b(j) - a(i)\}.$$

Certainly, filtered modules and their homomorphisms form a category. Consequently, we may speak, in particular, about isomorphisms between filtered modules.

LEMMA 1. *Let $a : [1, p] \rightarrow \mathbb{Z}_+$ and $b : [1, q] \rightarrow \mathbb{Z}_+$ be two twisting functions. If*

$$S^p[-a] \simeq S^q[-b],$$

then $p = q$ and $a = b$ (up to permutation).

Proof. That $p = q$ is obvious. Proving the second equality, we may assume that a and b are increasing functions. Suppose that $a \neq b$, and let i be the smallest number such that $a(i) \neq b(i)$. Say that $a(i) > b(i)$. Letting $d = a(i)$, we have:

$$S^p[-a]_{\leq d} \simeq S^p[-b]_{\leq d}.$$

But the left side here is equal to

$$S_{\leq a(1)-d} \oplus \cdots \oplus S_{\leq a(i-1)-d} \oplus \mathbb{F} \oplus \cdots$$

and the right side is

$$S_{\leq b(1)-d} \oplus \cdots \oplus S_{\leq b(i-1)-d}.$$

We get a contradiction. \square

The category of filtered modules is not abelian. Nevertheless, we may speak about exact sequences in it. Call a complex of filtered modules

$$(F_l, (F_{l,\leq d})) \xrightarrow{\delta_l} \cdots \xrightarrow{\delta_3} (F_1, (F_{1,\leq d})) \xrightarrow{\delta_1} (F_0, (F_{0,\leq d}))$$

exact if the sequence

$$F_{l,\leq d} \xrightarrow{\delta_l} \cdots \xrightarrow{\delta_3} F_{1,\leq d} \xrightarrow{\delta_1} F_{0,\leq d}$$

is exact for all $d \geq 0$.

LEMMA 2. *If a complex of filtered modules*

$$(F_l, (F_{l,\leq d})) \xrightarrow{\delta_l} \cdots \xrightarrow{\delta_2} (F_1, (F_{1,\leq d})) \xrightarrow{\delta_1} (F_0, (F_{0,\leq d}))$$

is exact, then the complex of modules

$$F_l \xrightarrow{\delta_l} \cdots \xrightarrow{\delta_2} F_1 \xrightarrow{\delta_1} F_0$$

also is exact.

Proof. This is obvious because $F_i = \lim_{d \rightarrow 0} F_{i,\leq d}$ (and because the direct limit functor is an exact functor). \square

Definition. Let $G = (G_l, \dots, G_1)$ be a polynomial complex, and let $q \times (p_l, \dots, p_1)$ be its size. Define the degree functions

$$a_i : [1, p_i] \rightarrow \mathbb{Z}_+, \quad i = 1, \dots, l$$

recursively as follows. Put $a_0 = 0$, and if a_i is defined, define a_{i+1} to be

$$a_{i+1} = \deg_{a_i}(G_{i+1}).$$

Call (a_l, \dots, a_1) the column degree table of G . The polynomial complex G gives rise to the following complex of filtered modules

$$(2.1) \quad 0 \rightarrow S^{p_l}[-a_l] \xrightarrow{G_l} \cdots \xrightarrow{G_2} S^{p_1}[-a_1] \xrightarrow{G_1} C[0] \rightarrow 0.$$

We say that G has the PD (predictable degree) property if this complex is exact.

The following example justifies the above definition.

Example. Assume $n = 1$. Following Forney [5], a polynomial matrix $G \in S^{q \times p}$ is said to have the PD property if, for every $f \in S^p$,

$$\deg(Gf) = \deg_a(f),$$

where a is the column degree function of G . For each $d \geq 0$, G determines a linear map

$$S^p[-a]_{\leq d} \rightarrow C_{\leq d},$$

and it is easily seen that G has the PD property in the sense of Forney if and only if all these linear maps are bijective.

Let C be a convolutional code of length q . Define the Hilbert function of C as

$$\text{HF}(C, d) = \dim_{\mathbb{F}}(C_{\leq d}), \quad d \in \mathbb{Z}_+.$$

This can be easily computed from the column degree table of a polynomial resolution of C having the PD property. Indeed, if (G_l, \dots, G_1) is such a resolution and if (a_l, \dots, a_1) is its column degree table, then, for each $d \geq 0$,

$$(2.2) \quad 0 \rightarrow S^{p_l}[-a_l]_{\leq d} \xrightarrow{G_l} \cdots \xrightarrow{G_2} S^{p_1}[-a_1]_{\leq d} \xrightarrow{G_1} C_{\leq d} \rightarrow 0$$

is an exact sequence of finite-dimensional linear spaces. As is known, the dimension of the space of polynomials of degree $\leq d$, where $d \in \mathbb{Z}$, is equal to $\binom{d+n}{n}$ (with

the convention that $\binom{d+n}{n} = 0$ when $d \leq -1$. It immediately follows from (2) therefore that

$$\text{HF}(C, d) = \sum_{i=1}^l (-1)^{i-1} \sum_j \binom{d - a_i(j) + n}{n}.$$

Remarks. Hilbert functions were introduced by Hilbert in the context of graded finitely generated modules. For one-dimensional convolutional codes, they have been defined in McEliece and Stanley [12]. Notice that the above expression for Hilbert function is a generalization of that given in [Corollary 3.2, 13].

3. The homogenization and the leading term complex. According to Lemma 2, the polynomial complexes having the PD property are polynomial resolutions necessarily. The converse is not true, and the goal of this section is to obtain a test to establish whether a polynomial resolution has the predictable degree property or not.

We need to recall the notion of graded modules.

Let M be a module over S or T . A gradation on M is a sequence

$$M_0, M_1, M_2, \dots$$

of \mathbb{F} -linear subspaces of M such that

$$M = \bigoplus M_d \quad \text{and} \quad D_k M_d \subseteq M_{d+1} \quad \forall k, d.$$

A module equipped with a gradation is called a graded module.

Example. Let R be either S or T . A twisting function a of length p determines on R^p the gradation consisting of the spaces

$$R^p(-a)_d = \{f \in S^p \mid \deg(f_i) = d - a(i)\} \quad (d \geq 0).$$

The module R^p equipped with this gradation will be denoted by $R^p(-a)$.

A homomorphism of graded modules $(M, (M_d)) \rightarrow (N, (N_d))$ is a homomorphism $u : M \rightarrow N$ such that

$$\forall d \geq 0, \quad u(M_d) \subseteq N_d.$$

Graded modules form an abelian category, and one therefore has the notion of exact sequences. It is worth noting that a complex of graded modules

$$(F_l, (F_{l,d})) \xrightarrow{\delta_l} \dots \xrightarrow{\delta_2} (F_1, (F_{1,d})) \xrightarrow{\delta_1} (F_0, (F_{0,d}))$$

is exact if and only if the sequence of linear spaces

$$F_{l,d} \xrightarrow{\delta_l} \dots \xrightarrow{\delta_2} F_{1,d} \xrightarrow{\delta_1} F_{0,d}$$

is exact for all $d \geq 0$.

The homogenization in degree d is the bijective linear map

$$S_{\leq d} \rightarrow T_d$$

defined by

$$f(D) \mapsto D_0^d f(D/D_0).$$

(Here and below D/D_0 means $(D_1/D_0, \dots, D_n/D_0)$.)

(*Warning:* It is essential to indicate the "d". For instance, the homogenization in degree 4 of the polynomial $2D_1^3 D_n + 1$ is $2D_1^3 D_n + D_0^4$ and the homogenization in degree 5 is $2D_0 D_1^3 D_n + D_0^5$.)

Let $C \subseteq S^p$ be a convolutional code. The homogenization C^H of C is defined to be

$$C^H = \bigoplus_{d \geq 0} C_d^H,$$

where C_d^H is the image of $C_{\leq d} = C \cap \mathbb{F}[s]_{\leq d}^p$ under the homogenization operator $S_{\leq d}^p \rightarrow T_d^p$. This is a "homogeneous convolutional code" in T^p .

Definition Let $G = (G_l, \dots, G_1)$ be a polynomial complex, and let $q \times (p_l, \dots, p_1)$ be its size and (a_l, \dots, a_1) the column degree.

a) The homogenization of G is the sequence $G^H = (G_l^H, \dots, G_1^H)$ of homogeneous polynomial matrices, where $G_k^H = D_0^{-a(k)} G_k(D/D_0) D_0^{a(k+1)}$.

b) The leading term complex of G is the sequence $G^L = (G_l^L, \dots, G_1^L)$ of homogeneous polynomial matrices, where G_k^L is defined as follows. The (i, j) entry of G_k^L is the homogeneous $(a_{k+1}(j) - a_k(i))$ -th part of the (i, j) entry of G_k .

These two sequences give rise respectively to the following complexes of graded modules:

$$(3.1) \quad 0 \rightarrow T^{p_l}(-a_l) \xrightarrow{G_l^H} \dots \xrightarrow{G_2^H} T^{p_1}(-a_1) \xrightarrow{G_1^H} T^q(0)$$

and

$$(3.2) \quad 0 \rightarrow S^{p_l}(-a_l) \xrightarrow{G_l^L} \dots \xrightarrow{G_2^L} S^{p_1}(-a_1) \xrightarrow{G_1^L} S^q(0).$$

We remark that

$$G^L(D) = G^H(0, D),$$

that is, G^L is obtained from G^H by replacing D_0 by 0.

THEOREM 1. *Let $G = (G_l, \dots, G_1)$ be a polynomial complex, and let $q \times (p_l, \dots, p_1)$ be its size and (a_l, \dots, a_1) the column degree. The following three conditions are equivalent:*

- (a) G has the PD property;
- (b) $\text{Im} G_1^H = C^H$ and the complex (3) is exact;
- (c) G is a polynomial resolution and the complex (4) is exact.

Proof. (a) \Leftrightarrow (b) This is obvious since the complex (2) is isomorphic to the complex

$$0 \rightarrow T^{p_l}(-a_l)_d \xrightarrow{G_l^H} \dots \xrightarrow{G_2^H} T^{p_1}(-a_1)_d \xrightarrow{G_1^H} C_d^H \rightarrow 0.$$

(b) \Rightarrow (c) We have an exact sequence

$$0 \rightarrow T^{p_l}(-a_l) \xrightarrow{G_l^H} \dots \xrightarrow{G_2^H} T^{p_2}(-a_2) \xrightarrow{G_1^H} T^q \rightarrow T^q/C^H.$$

We claim that D_0 is not a zero divisor on T^q/C^H . Suppose that $u \in T_d^q$ is such that $D_0 u \in C_{1+d}^H$. Then $u(1, D) \in C$. Since $u(1, D)$ has degree $\leq d$, we have $u(1, D) \in C_{\leq d}$. Clearly, u is the d -homogenization of $u(1, D)$, and therefore belongs to C_d^H . Using Corollary 1 in [10], we can see that the sequence

$$0 \rightarrow T^{p_l}(-a_l) \xrightarrow{G_l^H} T^{p_{l-1}}(-a_{l-1}) \rightarrow \cdots \xrightarrow{G_1^H} T^q.$$

remains exact after tensoring it by $T/D_0 T = S$. Notice that replacing D_0 by 0 in each entry of G_i^H , we get G_i^L . This means that

$$G_i^H \otimes T/D_0 T = G_i^L.$$

(b) \Rightarrow (a) Let $d \geq 0$. We have to show that the sequence

$$0 \rightarrow S^{p_l}[-a_l]_{\leq d} \xrightarrow{G_l} \cdots \xrightarrow{G_2} S^{p_1}[-a_1]_{\leq d} \xrightarrow{G_1} C_{\leq d} \rightarrow 0$$

is exact. For $1 \leq i \leq l-1$, we set

$$X_i = \text{Ker}(S^{p_i}[-a_i]_{\leq d} \xrightarrow{G_i} S^{p_{i-1}}[-a_{i-1}]_{\leq d});$$

if $i = 0$, define X_i to be $C_{\leq d}$.

Take any $x \in X_i$. By the hypothesis, there exists $y \in S^{p_{i+1}}$ such that $G_{i+1}y = x$. If $\deg_{a_{i+1}}(y) \leq d$, we are done. If $k = \deg_{a_{i+1}}(y) > d$, write

$$y = y^L + y'$$

with $y^L \in S^{p_{i+1}}(-a_{i+1})_k$ and $y' \in S^{p_{i+1}}[-a_{i+1}]_{\leq k-1}$. It is clear that $G_{i+1}^L y^L = 0$. Hence, by the hypothesis, $G_{i+2}^L z = y^L$ for some $z \in S^{p_{i+2}}(-a_{i+2})_k$. Consider the element $y_1 = y - G_{i+2}z$. It has a_{i+1} -degree $< k$ and

$$G_{i+1}y_1 = G_{i+1}y - G_{i+1}G_{i+2}z = G_{i+1}y = x.$$

Using induction, we find that there exists an element in $S^{p_{i+1}}[-a_{i+1}]_{\leq d}$ that goes to x .

The proof is complete. \square

Definition. Let $G = (G_1, \dots, G_l)$ be a polynomial complex, and let $q \times (p_l, \dots, p_1)$ be its size and (a_l, \dots, a_1) the column degree. Say that G is (column) reduced if the complex (4) is exact.

We thus have the following statement.

COROLLARY 1. *A polynomial resolution has the PD property if and only if it is reduced.*

Remark. In dimension 1, if G is a full column rank polynomial matrix with degree function a , then G^L is equal to the leading coefficient matrix multiplied by the diagonal matrix with $D^{a(i)}$ on the diagonal. For example, if

$$G = \begin{bmatrix} 2D^3 + D + 1 & D^2 - 10 \\ D^2 - 5 & D + 4 \\ 3D^4 + 7D & D^2 + 1 \end{bmatrix},$$

then the column degree is equal to $(4, 2)$, and we have

$$G^L = \begin{bmatrix} 0 & D^2 \\ 0 & 0 \\ 3D^4 & D^2 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \\ 3 & 1 \end{bmatrix} \begin{bmatrix} D^4 & 0 \\ 0 & D^2 \end{bmatrix}.$$

Therefore, the above corollary should be regarded as a generalization of the classical Forney's theorem stating that a full column rank polynomial matrix has the PD property if and only if its leading coefficient matrix has full column rank.

4. Minimal reduced polynomial resolutions, and Forney tables. A priori is not clear that every convolutional code possesses reduced polynomial resolutions. The issue of minimality also is not obvious. (In dimension 1, reduced polynomial matrices automatically are minimal.) In this section, we shall see that for every convolutional code there exists a minimal reduced polynomial resolution and that such a resolution is uniquely determined up to equivalence.

Let $(M, (M_{\leq d}))$ be a filtered module. If $d \geq 0$, then

$$M_{\leq d-1} + D_1 M_{\leq d-1} + \cdots + D_n M_{\leq d-1}$$

is the part of $M_{\leq d}$ that comes from $M_{\leq d-1}$ and should be regarded as the trivial part of $M_{\leq d}$. It is natural therefore to consider the quotient

$$\frac{M_{\leq d}}{M_{\leq d-1} + D_1 M_{\leq d-1} + \cdots + D_n M_{\leq d-1}},$$

which is a linear space over \mathbb{F} . Denote it by $\Gamma_d(M, (M_{\leq d}))$.

Example. There holds

$$\Gamma_d(S[-k]) = \begin{cases} \mathbb{F} & \text{when } d = k; \\ \{0\} & \text{when } d \neq k. \end{cases}$$

Let $u : (M, (M_{\leq d})) \rightarrow (N, (N_{\leq d}))$ be a homomorphism of filtered modules. We say that u is minimal if it satisfies the following two conditions:

- 1) $u : M_{\leq d} \rightarrow N_{\leq d}$ is surjective $\forall d \geq 0$;
- 2) $\Gamma_d(u) : \Gamma_d(M, (M_{\leq d})) \rightarrow \Gamma_d(N, (N_{\leq d}))$ is bijective $\forall d \geq 0$.

LEMMA 3. *Let $p \geq 1$, and let C be a (nontrivial) convolutional code in S^p . For any twisting function $a : [1, p] \rightarrow \mathbb{Z}_+$, there exists a polynomial matrix G such that*

$$G : S^q[-b] \rightarrow C[-a],$$

where q is the column number and b the column a -degree of G , is minimal.

Proof. See Lemma 7 in [11]. \square

Any G satisfying the conditions of the lemma is called a minimal a -representation of C . In the case when $a = 0$, we simply say "minimal representation".

An exact sequence of filtered modules

$$(F_l, (F_{l, \leq d})) \xrightarrow{\delta_l} \cdots \xrightarrow{\delta_2} (F_1, (F_{1, \leq d})) \xrightarrow{\delta_1} (F_0, (F_{0, \leq d}))$$

is said to be minimal if δ_1 is minimal and, for each $i \geq 2$, the homomorphism

$$\delta_i : (F_i, (F_{i, \leq d})) \rightarrow (\text{Ker} \delta_{i-1}, (\text{Ker} \delta_{i-1} \cap F_{i-1, \leq d}))$$

also is minimal.

Definition. Let $G = (G_1, \dots, G_l)$ be a reduced polynomial resolution, and let $q \times (p_l, \dots, p_1)$ be its size and (a_l, \dots, a_1) the column degree. Say that G is minimal if the sequence (1) of filtered modules is minimal.

One constructs a minimal reduced polynomial resolution step by step, using the previous lemma. Assume we have a convolutional code $C \subseteq S^q$. Choose a minimal representation G_1 of C . Let C_1 be the kernel of $G_1 : S^{p_1} \rightarrow C$, where p_1 is the column number of G_1 . Letting a_1 denote the degree function of G_1 , choose next a minimal a_1 -representation G_2 of C_1 . If we continue this way the process will terminate.

THEOREM 2. *Every convolutional code has a minimal reduced polynomial resolution.*

Proof. This is an immediate consequence of the "graded" Hilbert syzygy theorem. (See Theorem 4.15 in Lang [9] and Theorem 1 in [11].) \square

Let $G = (G_l, \dots, G_1)$ and $G' = (G'_l, \dots, G'_1)$ be two reduced polynomial resolutions. Let $q \times (p_l, \dots, p_1)$ and $q \times (p'_l, \dots, p'_1)$ be their sizes, and let (a_l, \dots, a_1) and (a'_l, \dots, a'_1) be their column degree tables. We say that G and G' are equivalent if there exist isomorphisms

$$U_i : S^{p_i}[-a_i] \rightarrow S^{p'_i}[-a'_i], \quad i = 1, \dots, l$$

such that

$$G'_1 U_1 = G_1, \quad G'_2 U_2 = U_1 G_2, \dots, \quad G'_l U_l = U_{l-1} G_l.$$

It is immediate from Lemma 1 that equivalent reduced polynomial resolutions have the same size and the same column degree table.

THEOREM 3. *Any two minimal reduced polynomial resolutions of a convolutional code are equivalent.*

Proof. This is an immediate consequence of the theorem about uniqueness of minimal graded free resolutions. (See Theorem 6.3.13 in Cox, Little and O'Shea [2], Theorem 1.6 in Eisenbud [3], and Theorem 1 in [11].) \square

The above two theorems permit us to give the following definition.

Definition. Let $C \subseteq S^q$ be a convolutional code, and let $G = (G_l, \dots, G_1)$ be any its minimal reduced polynomial resolution. We define the rate of C to be $(p_l, \dots, p_1)/q$, where (p_l, \dots, p_1) is the size of G . Next, we define the Forney table of C to be the column degree table of G . The maximum value of the degree function of G_1 is called the *memory* of the code.

PROPOSITION 1. *Let C be a convolutional code, and let m be its memory. Then C can be recovered from the knowledge of $C_{\leq m}$.*

Proof. Let G_1 be a minimal representation of C , and let p_1 its column number, a_1 the degree function and m the memory. For $d > m$, we have

$$\Gamma_d(S^{p_1}[-a_1]) = 0.$$

Because $G_1 : S^{p_1}[-a_1] \rightarrow C$ is minimal, we get that $\Gamma_d(C) = 0$ for all $d > m$. In other words, for all such d , we have

$$C_{\leq d} = C_{\leq d-1} + D_1 C_{\leq d-1} + \dots + D_n C_{\leq d-1}.$$

It follows that knowing $C_{\leq m}$, we can find all $C_{\leq d}$ with $d > m$. This completes the proof since, for any N ,

$$C = \bigcup_{d \geq N} C_{\leq d}.$$

\square

Closing the section, we want to present a simple test for establishing whether a given reduced polynomial resolution is minimal or not.

PROPOSITION 2. *Let $G = (G_l, \dots, G_1)$ be a reduced polynomial resolution. If $l = 1$, then G is minimal. If $l \geq 2$, the G is minimal if and only if none of the nonzero entries of the matrices G_2^L, \dots, G_l^L are scalars from \mathbb{F} .*

Proof. The case $l = 1$ is obvious. The resolution G is minimal if and only if the sequence of graded free modules (3) is minimal. (The reader is referred to Eisenbud

[3] for the notion of minimal graded free resolutions.) By Corollary 1.5 in [3], (3) is minimal if and only if the scalar matrices

$$G_k^H(0, 0, \dots, 0), \quad k = 2, \dots, l$$

are zero. This completes the proof since

$$G_k^L(0, \dots, 0) = G_k^H(0, 0, \dots, 0).$$

□

5. Observability. A desirable property from the point of view of coding is observability.

A convolutional code $C \subseteq S^q$ is called observable if the quotient module S^q/C is torsion free. As is known, a finitely generated module is torsion free if and only if it can be embedded into a free module of finite rank. It follows that C is observable if and only if it can be described through

$$C = \{f \in S^q \mid Hf = 0\},$$

where $H \in S^{\bullet \times q}$ is a polynomial matrix, called a parity check matrix or a syndrome former of C .

For an irreducible polynomial λ in $S = \mathbb{F}[D]$, let $\mathbb{F}(\lambda)$ denote the integral domain $\mathbb{F}[s]/\lambda\mathbb{F}[s]$. If G is a polynomial matrix, define G/λ to be its reduction modulo the principal ideal $\lambda\mathbb{F}[s]$.

We have the following proposition.

PROPOSITION 3. *Let $C \subseteq S^q$ be a convolutional code, and let (G_l, \dots, G_1) be its polynomial resolution of size (p_l, \dots, p_1) , say. Then C is observable if and only if the sequence*

$$0 \rightarrow \mathbb{F}(\lambda)^{p_l} \xrightarrow{G_l/\lambda} \dots \rightarrow \mathbb{F}(\lambda)^{p_1} \xrightarrow{G_1/\lambda} \mathbb{F}(\lambda)^q$$

is exact for every irreducible polynomial λ .

Proof. See Theorem 1 in [10]. □

Remark. In dimension 1, the statement is well-known in linear systems theory, where it is named as the Popov-Belevich-Hautus test of controllability.

REFERENCES

- [1] C. Charoenlarnopparut, "Applications of Gröbner bases to the structural description and realization of multidimensional convolutional code", *Science Asia*, vol. 35, pp. 95-105, 2009.
- [2] D.A. Cox, J. Little and D. O'Shea, *Using Algebraic Geometry*. New York, Springer-Verlag, 2005.
- [3] D. Eisenbud, *The Geometry of Syzygies: A Second Course in Algebraic Geometry and Commutative Algebra*. New York, Springer-Verlag, 2005.
- [4] E. Fornasini and M.E. Valcher, "Algebraic aspects of two-dimensional convolutional codes", *IEEE Trans. Inform. Theory*, vol. 40, pp. 1068-1082, 1994.
- [5] G.D. Forney Jr., "Convolutional codes I: Algebraic structure", *IEEE Trans. Inform. Theory*, vol. IT-16, pp. 720-738, 1970.
- [6] H. Gluesing-Luerssen, J. Rosenthal and P. Weiner, "Duality between multidimensional convolutional codes and systems", in *Advances in mathematical systems theory*, F. Colonius, U. Helmke, D. Pritzel-Wolters and F. Wirth, Eds. Boston, MA, 2001, pp. 135-150.
- [7] P. Jangisarakul and C. Charoenlarnopparut, "Algebraic decoder of a multidimensional convolutional code: constructive algorithms for determining syndrome decoder and decoder matrix based on Gröbner basis", *Multidim. Syst. Sign. Process.*, vol. 22, pp. 67-81, 2011.

- [8] B. Kitchens, "Multidimensional convolutional codes", *SIAM J. Discrete Math.*, vol. 15, pp. 367-381, 2002.
- [9] S. Lang, *Algebra*. New York, Springer-Verlag, 2002.
- [10] V. Lomadze, "PBH test for multivariate LTID systems", *Automatica*, vol. 49, pp. 2933-2937, 2013.
- [11] V. Lomadze, ""Reduced polynomial matrices" in several variables", *SIAM J. Control Optim.*, vol. 51, pp. 3258-3273, 2013.
- [12] R.J. McEliece and R.P. Stanley, "The general theory of convolutional codes", *The Telecommunications and Data Acquisition Progress Report 42-113*, pp. 89-98, January-March 1993.
- [13] D. Napp Avelli, C. Perea and R. Pinto, "Input-state-output representations and constructions of finite-support 2D convolutional codes", *Advances in Mathematics of Communications*, vol. 4, pp. 533-545, 2010.
- [14] D. Napp Avelli, C. Perea and R. Pinto, "Column distances for 2D-convolutional codes", *Proceedings of the 19th International Symposium on MTNS*, Budapest, Hungary, 2010.
- [15] M.E. Valcher and E. Fornasini. "On 2D finite support convolutional codes: an algebraic approach", *Multidim. Syst. Sign. Process.*, vol. 5, pp. 231-243, 1994.
- [16] P. Weiner. "Multidimensional Convolutional Codes", Ph.D. dissertation, University of Notre Dame, USA, 1998.
- [17] E. Zerz, "On multidimensional convolutional codes and controllability properties of multidimensional systems over finite rings", *Asian Journal of Control*, vol. 12, pp. 117-236, 2010.